



피해갈 수 없는 탐지력

# 알약

월간 보안동향 보고서

## 목차

### Part I. 11 월의 악성코드 통계

1. 악성코드 통계.....	2
(1) 감염 악성코드 Top 15.....	2
(2) 카테고리별 악성코드 유형.....	3
(3) 카테고리별 악성코드 비율 전월 비교.....	3
(4) 월별 피해 신고 추이.....	4
(5) 월별 악성코드 DB 등록 추이.....	4
2. 악성코드 이슈 분석 - “백신 제품의 정상 동작을 방해하는 Anti-AV” .....	5
3. 허니팟/트래픽 분석.....	9
(1) 상위 Top 10 포트 .....	9
(2) 상위 Top 5 포트 월별 추이 .....	9
(3) 악성 트래픽 유입 추이.....	10
4. 스팸메일 분석.....	11
(1) 일별 스팸 및 바이러스 통계 현황.....	11
(2) 월별 통계 현황.....	11
(3) 스팸 메일 내의 악성코드 현황.....	12

### Part II. 11 월의 보안 이슈 돋보기

1. 11 월의 보안 이슈 .....	13
2. 11 월의 취약점 이슈.....	15



Part I 11월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2010년 11월 1일 ~ 2010년 11월 30일]

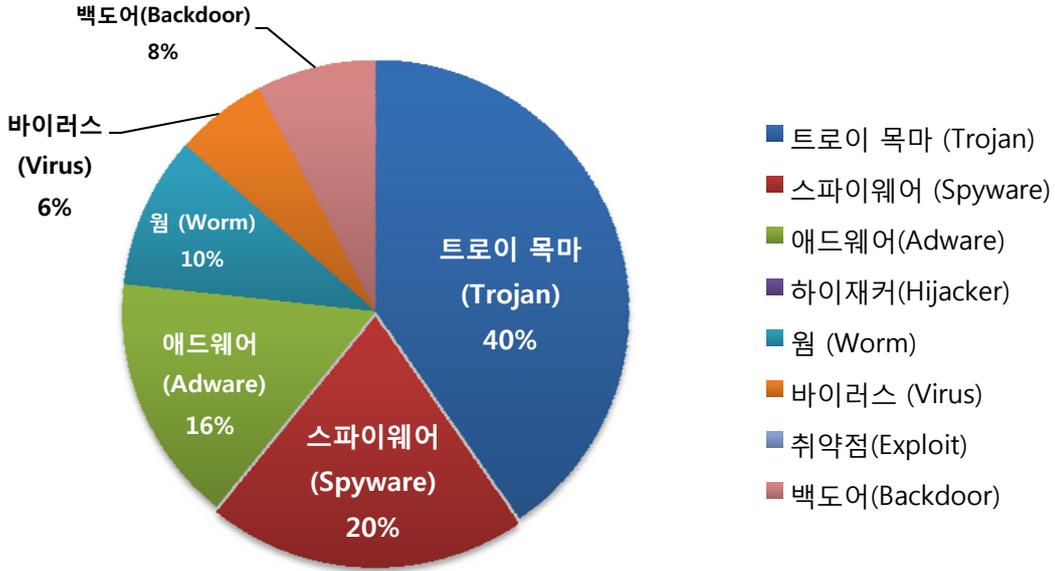
순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑ 4	V.DWN.el.39xxxx	Trojan	50,987
2	↑ 9	V.TRJ.Patched.imm	Trojan	38,343
3	↑ 1	S.SPY.Lineag-GLG	Spyware	38,123
4	New	Variant.Fosniw.1	Trojan	35,217
5	New	Variant.Backdoor.7	Backdoor	32,684
6	↑ 2	V.DWN.Agent.Pinsearch	Trojan	27,461
7	New	S.SPY.OnlineGames.imm	Spyware	26,706
8	New	Variant.Adware.Oso.1	Adware	25,292
9	↓ 8	Win32.Parite.B	Virus	24,948
10	New	S.SPY.WoWar	Spyware	22,227
11	↓ 5	A.ADV.BHO.IESearch	Adware	21,852
12	New	Variant.Palevo.11	Worm	21,214
13	New	Adware.Generic.146751	Adware	20,706
14	↓ 1	V.WOM.Conficker	Worm	20,425
15	New	Trojan.Zlob.1.Gen	Trojan	20,401

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다. 11월의 감염 악성코드 TOP 15는 V.DWN.el.39xxxx가 50,987건으로 TOP 15 중 1위를 차지하였으며, V.TRJ.Patched.imm이 38,343건으로 2위, S.SPY.Lineag-GLG가 38,123건으로 3위를 차지하였다. 이외에도 11월에 새로 Top 15에 진입한 악성코드는 8종이다. 11월에는 MS Internet Explorer의 보안 취약점(CVE-2010-3962)를 이용한 악성코드 유포 사례가 가장 많이 보고되었다. 또한 정상적인 imm32.dll 파일을 변조된 악성 파일로 교체시키는 역할과 백신 무력화 기능을 수행하며, 온라인 게임 계정 유출을 위한 목적으로 제작되었다.

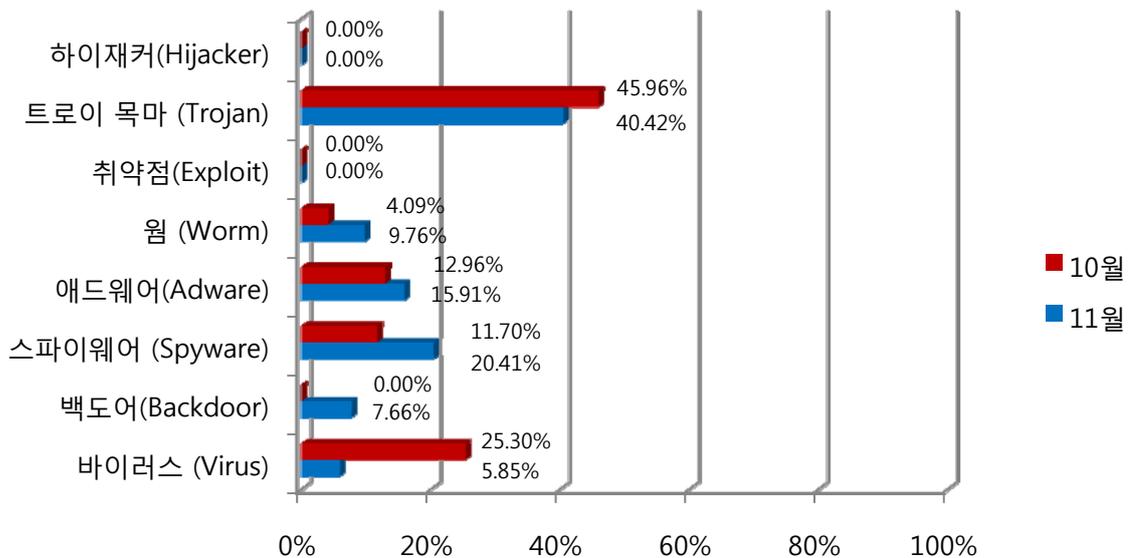


## (2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 이번달에도 트로이 목마(Trojan)가 40%로 가장 많은 비율을 차지하였고, 전달에 비해 바이러스(Virus) 비율은 6%로 크게 감소하였다. (19% 비율 ↓)  
 10월 통계의 1, 2위를 차지한 파일 감염형 바이러스 Parite(Win32.Parite.B, V.TRJ.Parite.Gen)가 진정 국면에 접어들어 바이러스(Virus) 비율이 크게 감소한 것으로 보여지며, 11월에는 IE 취약점을 이용한 스파이웨어(Spyware)의 유포로 스파이웨어 비율이 증가(8%)하였다.

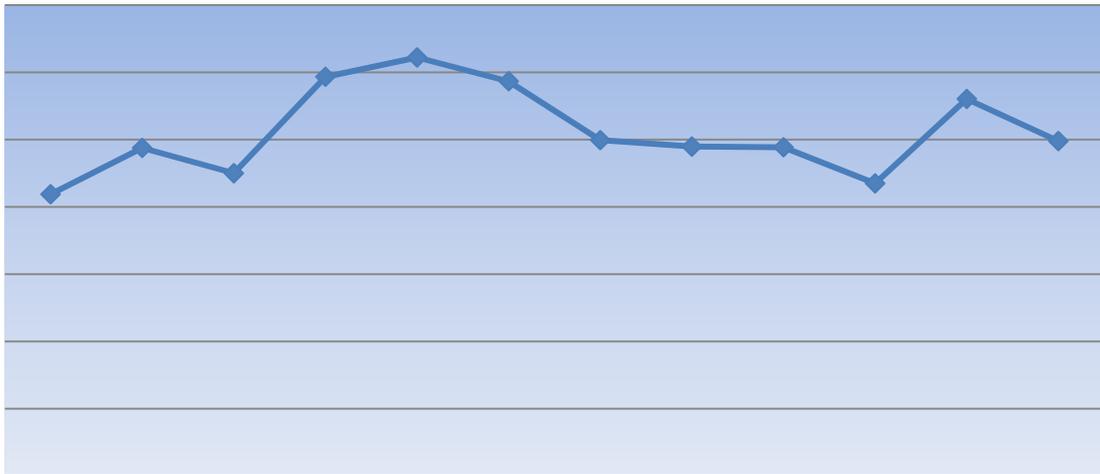
## (3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이 목마(Trojan)와 바이러스(Virus)가 전달에 비해 감소하였으며, 대부분의 다른 악성코드는 비율이 증가했음을 알 수 있다. (바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

#### (4) 월별 피해 신고 추이

[2009년 12월 ~ 2010년 11월]



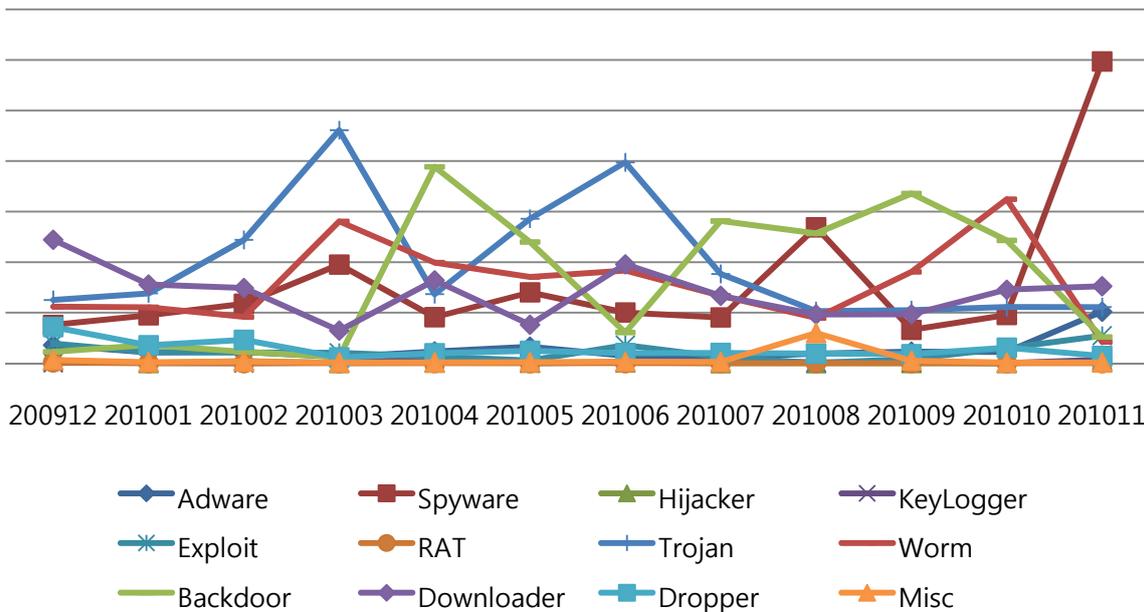
12월 1월 2월 3월 4월 5월 6월 7월 8월 9월 10월 11월

※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 11월의 경우 전달(10월)보다 신고 건수가 다시 감소하였다.

#### (5) 월별 악성코드 DB 등록 추이

[2009년 12월 ~ 2010년 11월]



200912 201001 201002 201003 201004 201005 201006 201007 201008 201009 201010 201011

◆ Adware      ■ Spyware      ▲ Hijacker      × KeyLogger  
✱ Exploit      ● RAT      + Trojan      — Worm  
— Backdoor      ◇ Downloader      ■ Dropper      ▲ Misc

11월은 스파이웨어(Spyware) 계열의 악성코드 변종이 가장 많이 등록 되었으며, 다음으로 다운로드 악성코드(Downloader)가 많이 등록 되었다. 이번 달 스파이웨어는 MS Internet Explorer 취약점(CVE-2010-3962)를 이용한 온라인 게임 계정 탈취와 관련하여 DB 등록이 급증하였다.

## Part I 11월의 악성코드 통계

## 2. 악성코드 이슈 분석 - "백신 제품의 정상 동작을 방해하는 Anti-AV"

예전부터 악성코드와 Anti-Virus(이하 AV)의 싸움은 계속 되어왔다.

기존의 악성코드들은 AV로부터 자신을 보호하기 위해 패킹이나 다형성 기법을 사용해 왔지만 최근에는 AV 파일이나 프로세스를 직접 공격하는 방법을 사용한다.

이번에 분석할 악성코드는 여러 AV 리스트를 가지고 있으며 프로세스에서 리스트에 있는 AV가 발견되면 해당 디렉토리에 있는 모든 EXE와 DLL 파일을 수정하여 제대로 된 AV 기능을 할 수 없게 만든다. 그 원리를 중점적으로 분석해 본다.

## 1) 악성코드 분석

이 악성코드는 DLL 파일 형태이고, 메인 스레드 외에 두 개의 스레드를 생성한다.

첫 번째 스레드는 특정 Anti-Virus 제품을 찾아서 실행을 막기 위해 파일을 변조하고, 두 번째 스레드는 인터넷에서 다른 악성코드를 다운로드하여 실행하는 일을 한다.

메인 스레드를 먼저 살펴보고 생성된 두 개의 스레드를 분석할 것이다.

## 2) 메인 스레드

메인 스레드는 세 가지 일을 한다. 파일 복사 후 DLL을 인젝션하고, 훅(Hook)을 설치하고, 스레드를 생성한다.

## ① 파일 복사

DLL이 실행중인 프로세스가 verclsid.exe인지 확인한다. 그리고 dwking.exe 프로세스가 실행 중이 아니면 %WINDOWS%\dwking.exe를 %WINDOWS%\notepad.exe로 복사하고 dwking.exe를 실행한다. 그리고 실행된 dwking.exe 프로세스에 dwking0.dll을 인젝션(Injection)해 DLL이 실행되도록 한다.

## ② 훅(Hook) 설치

DLL이 실행중인 프로세스가 dwking.exe 이라면 아래 레지스트리에서 값을 구하여 그 값이 DLL 파일명과 같으면 WH\_MOUSE와 WH\_CALLWNDPROC 메시지에 대해 훅을 설치 한다.

**CLSID\{90359234-04B2-A8D9-4A5D-F34B82327F64}\VckingDllModuleName**

VckingDllModuleName 외에도 VckingExeModuleName, VckingSobjEventName 값이 있으며, 이 값은 악성코드가 정보를 저장해두기 위한 용도로 사용한다.

## ③ 스레드 생성

Anti-Virus 실행파일을 변조하는 스레드와 악성코드를 다운로드하여 실행하는 스레드를 생성한다.

### 3) Anti-Virus 실행파일 변조 스텝

HLM의 SOFTWARE\Microsoft\Windows\CurrentVersion\Run에서 다음 리스트에 있는 이름으로 된 값이 있으면 삭제한다.

<b>LIVESRV.EXE</b>	<b>VCRMN.EXE</b>
<b>Update.exe</b>	<b>AHNSD.EXE</b>
<b>SUpdate.exe</b>	<b>autoup.exe</b>
<b>CCSVCHST.EXE</b>	<b>ALUSCHEDULERSVC.EXE</b>
<b>luall.exe</b>	<b>ASHDISP.EXE</b>
<b>setup.ovr</b>	<b>avast.setup</b>
<b>VisthUpd.exe</b>	<b>EKRN.EXE</b>
<b>updater.dll</b>	<b>eguiEpfw.dll</b>
<b>eguiEmon.dll</b>	<b>updater.dll</b>
<b>AVP.EXE</b>	<b>prupdate.ppl</b>
<b>AYAGENT.AYE</b>	<b>AYUpdate.aye</b>
<b>UFSEAGNT.EXE</b>	<b>SfFnUp.exe</b>
<b>UfUpdUi.exe</b>	<b>AVGNT.EXE</b>
<b>preupd.exe</b>	<b>update.exe</b>

그리고 위 리스트에 있는 프로세스가 실행 중인지 검사한다.

만약 실행 중이라면 파일을 변조하여 제대로 실행이 되지 않도록 한다.

이때 파일 관련 API(CreateFile, WriteFile)를 사용하여 실행중인 프로세스의 파일을 수정하려고 하면 에러가 발생한다. 그래서 파일 관련 API를 바로 사용하지 않고 파일 시스템에 직접 접근하여 파일을 변조하는 방법을 사용한다.

```
result = DeviceIoControl(hFile2, FSCTL_GET_RETRIEVAL_POINTERS, &InBuffer, 8u, &OutBuffer, 0x110u, &BytesReturned, 0);
if ( result )
{
    dwSizeLow = OutBuffer.Extents[0].Lcn.LowPart;
    dwSizeHigh = OutBuffer.Extents[0].Lcn.HighPart;
    GetFileSize(hFile2, 0);
    CloseHandle(hFile2);
    wsprintfA(&FileName, "WWW.WW%c:", *lpFileName);
    hFile = CreateFileA(&FileName, 0xC0000000u, 3u, 0, 3u, 0x20000000u, 0);
```

DeviceIoControl 함수에서 FSCTL\_GET\_RETRIEVAL\_POINTERS 컨트롤 코드를 사용하여 파일 시스템에서 해당 파일의 위치를 알아낸다.

그리고 파일 시스템인 WWW.Ww:c 의 핸들을 구해서 직접 쓰는 방법을 사용한다.

이 방법을 사용하면 실행중인 파일을 수정할 수 있다.

파일을 시작부터 0x200 크기만큼 변조한다. 이 부분은 PE 파일 포맷의 헤더 부분이다. 그 내용은 아래와 같다.

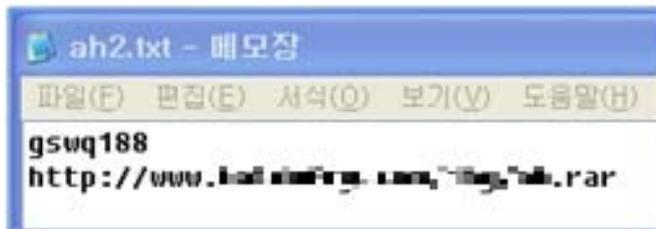




복호화 하려는 데이터에 복호화 키와 길에 관한 정보가 있다. 0x47은 복호화할 데이터의 길이이고 0x37은 복호화 키다. 0x37 다음 0xb3부터 0x47 크기만큼 복호화를 한다. 복호화 단순히 key를 빼는 방법을 사용한다. 복호화를 하면 두 개의 URL이 나오고 이것을 다운로드 하면 내부에 다른 URL 주소를 가지고 있다.

$$p = c - 0x37$$

복호화를 하면 두 개의 URL이 나오고 이것을 다운로드 하면 내부에 다른 URL 주소를 가지고 있다.



다시 이 URL을 다운로드 하여 파일을 실행한다.

### 5) 결론

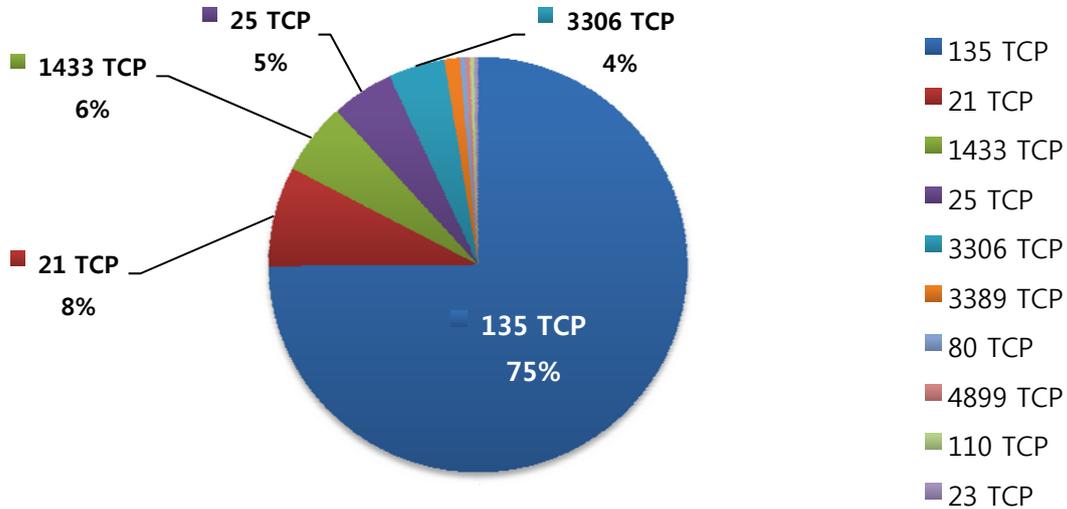
악성코드는 AV에 대항하기 위해 AV 파일을 변조하는 방법을 사용하였다. 그러자 AV는 자가보호라는 기능을 넣어서 AV 관련 파일을 변경하지 못하도록 하였다. 이처럼 악성코드와 AV의 싸움은 앞으로도 계속될 것으로 판단된다.



Part I 11월의 악성코드 통계

3. 허니팟/트래픽 분석

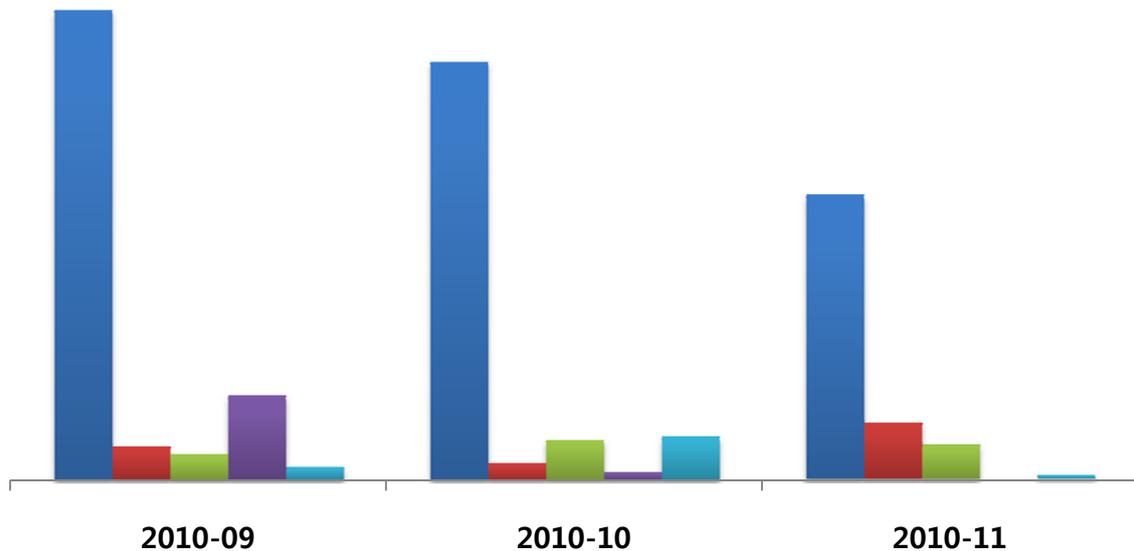
(1) 상위 Top 10 포트



11월에도 지속적으로 윈도우 자체의 취약점을 대상으로 한 TCP 135 포트 침입 시도가 가장 많았다. 지난달과 비교했을 경우 2% 감소하였고, TCP 21번에 대한 침입 시도가 전달에 비해 크게 증가하였다. (약 6% 비율 ↑) 또한 TCP 25 포트의 침입 시도가 3% 증가하였다.

(2) 상위 Top 5 포트 월별 추이

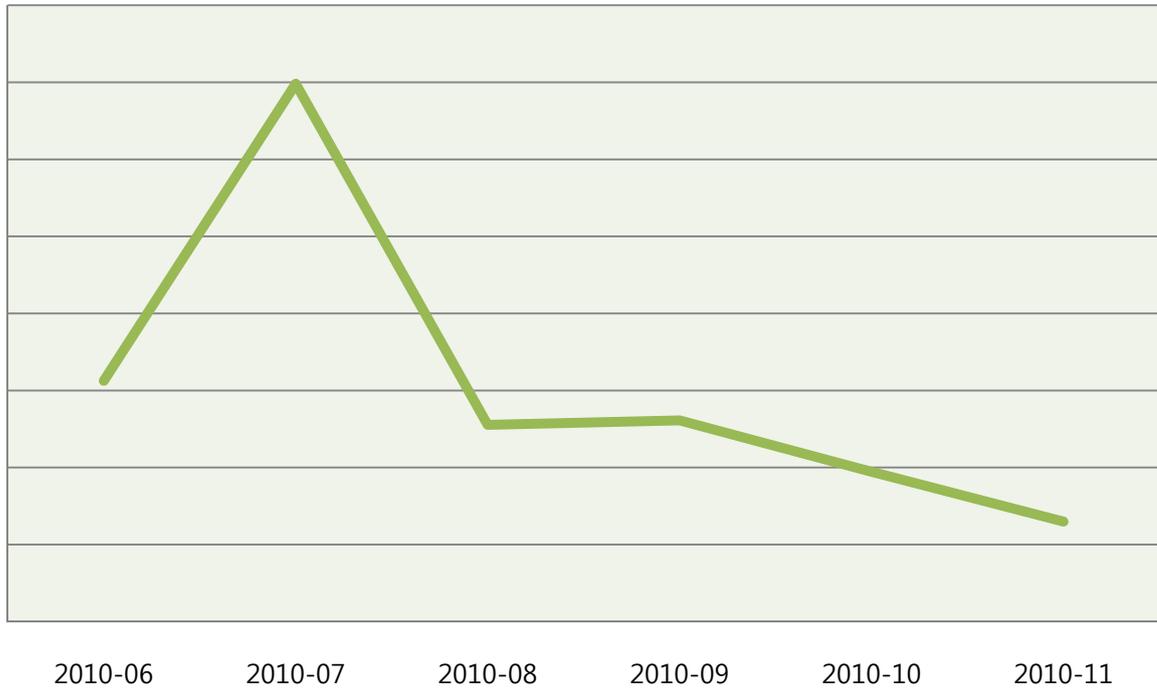
[2010년 9월 ~ 2010년 11월]



TCP 135번 포트에 대한 전체적인 추이는 감소 상태에 있지만 나머지 포트들의 경우 특정한 패턴이 나타나고 있지 않고 있다. 최근 서버들의 보안 패치 상태가 향상됨에 따라 특정 OS나 응용 프로그램의 보안 취약점을 노리는 공격 트래픽 보다는 사전 대입 방식으로 서버의 권한을 획득하고자 하는 악성 트래픽이 현재 대부분을 차지하고 있다.

### (3) 악성 트래픽 유입 추이

[2009년 6월 ~ 2010년 11월]



전체적인 악성 트래픽의 유입량은 전달에 비해 감소하였다.

이미 악성코드 유포 방식이 브라우저의 취약점을 악용하는 Drive-By Download (취약점 코드가 있는 웹사이트를 접속만 해도 브라우저에서 스스로 파일을 다운로드, 실행), 파일 공유를 위한 웹 서버에 정상 파일을 가장한 악성코드 업로드 및 실행 유도, 메신저 및 메일의 첨부 파일, 최근 SNS에서의 단축 URL 등을 통해 다양화 되고 있다.

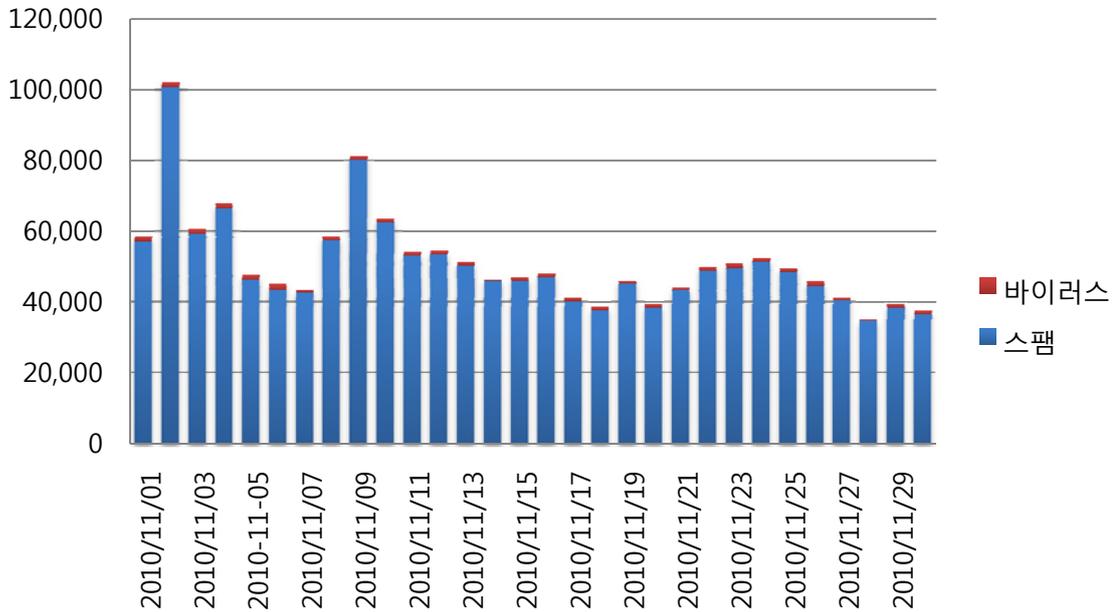
이에 따라 OS 및 응용 소프트웨어의 보안 취약점으로 인한 문제를 해결하기 위해서는 최신 보안 업데이트를 반드시 설치해야 하고, 악성코드의 감염을 예방하기 위해 최신 백신을 사용해야 한다.



Part I 11월의 악성코드 통계

3. 스팸 메일 분석

(1) 일별 스팸 및 바이러스 통계 현황

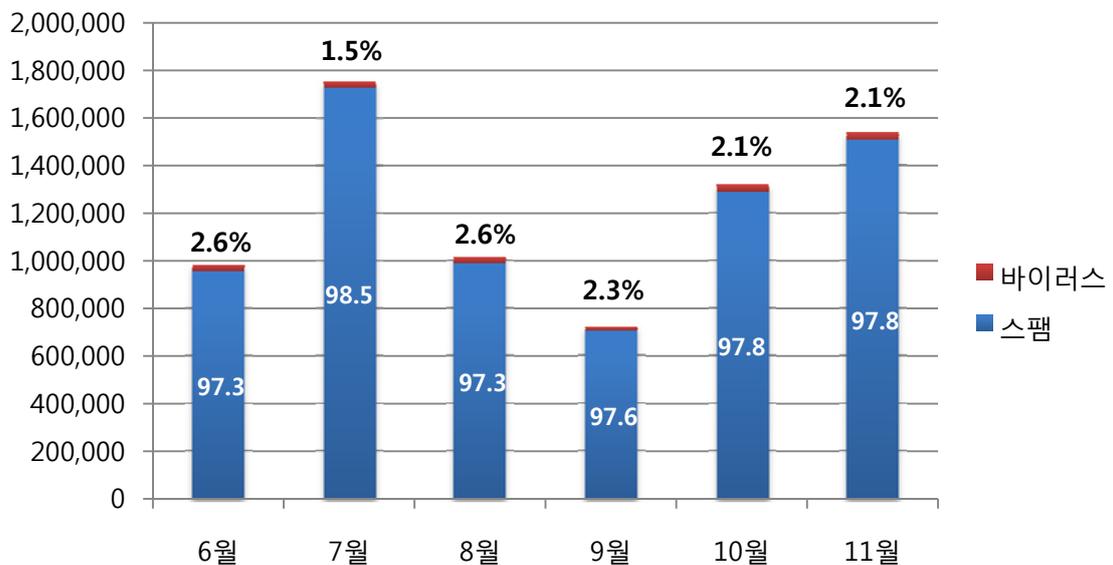


일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 11월에는 지방경찰청 사이버수사대와 G-20 이슈 문서, 노벨평화상 초청장, 광저우 아시안게임과 관련한 악성코드 이메일이 유포되었다.

이번 달 크리스마스 기간에는 연하장을 위장한 이메일 악성코드 유포가 많을 것으로 예측되고 있으며, 실제 12월 6일 국내에서 크리스마스 연하장을 위장한 이메일이 발견되었다.

(2) 월별 통계 현황

[2010년 6월 ~ 2010년 11월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다. 11월의 스팸 메일은 97.8%, 바이러스 메일은 2.1%를 차지하였다. 10월에 비해서는 비율의 변동이 없었으나 바이러스와 스팸메일을 포함한 전체적인 메일 수신량은 증가하였다.

### (3) 스팸 메일 내의 악성코드 현황

[2010년 11월 1일 ~ 2010년 11월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	12,3279	37.74%
2	W32/MyDoom-H	6,267	19.19%
3	Mal/ZipMal-B	4,320	13.23%
4	W32/Virut-T	2,509	7.68%
5	W32/Bagz-D	1,057	3.24%
6	W32/MyDoom-AJ	884	2.71%
7	W32/Autorun-BHX	764	2.34%
8	W32/MyDoom-Gen	686	2.10%
9	W32/Bagle-CF	586	1.79%
10	Troj/Invo-Zip	560	1.71%

스팸 메일 내의 악성코드 현황은 10월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Mytob-C가 37.74%로 1위를 차지하였다.

2위는 19.19%를 차지한 W32/MyDoom-H, 3위는 13.23%를 차지한 Mal/ZipMal-B이다.

11월에는 W32/MyDoom-AJ와 W32/Autorun-BHX 악성코드가 새롭게 순위에 등장하였으며, 1~5위까지는 전달과 비교해 변동이 없다.



Part II 11월의 이슈 돋보기

1. 11월의 보안 이슈

11월에는 스마트폰 모바일 백신 “알약 안드로이드 공개”, 내년 전 세계 IPv4 주소 신규 할당 중단, 10대 로우킥녀 학교 홈페이지 해킹, 지방경찰청 사이버수사대, 노벨평화상 초청장을 위장한 악성코드 이메일 유포 등 여러 이슈가 있었습니다.

• **이스트소프트 스마트폰 모바일 백신 “알약 안드로이드” 공개**

지난 11월 29일 ISEC 2010 통합 정보보호 구축전략 컨퍼런스에서 스마트폰 모바일 백신인 “알약 안드로이드(Android)”가 처음으로 공개되었습니다.

알약 안드로이드는 국내 무료 백신 사용자수 1위 “알약”의 보안 기술을 바탕으로, 안드로이드에 최적화된 모바일 백신입니다. 또한, 모바일 백신의 필수 기능인 악성 파일과 App에 대한 검사 및 치료 기능을 제공하며, App에 대한 안전 등급과 실시간 스팸(전화번호, 문자메시지) 알림/차단 서비스 같은 유용한 부가 기능을 함께 가지고 있습니다.

현재 안드로이드 마켓이나 알약 홈페이지에서 “알약 안드로이드”를 설치할 수 있습니다.

▣ 알약 안드로이드



스마트폰 보안 업그레이드

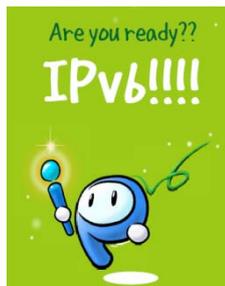
**알약 안드로이드**

- > 악성 파일 및 패키지 검사
- > App 안전 등급 제공으로 스마트폰 보안 강화
- > 실행중인 App 관리로 스마트폰 사용환경 최적화
- > 스팸 전화, 스팸 문자메시지를 실시간으로 차단 및 관리
- > 사용성을 고려한 쉽고 편리한 내구성
- > 터치 한 번으로 보안 기능을 간편하게 설정 및 적용

• **내년부터 전 세계 IPv4 주소 신규 할당 중단**

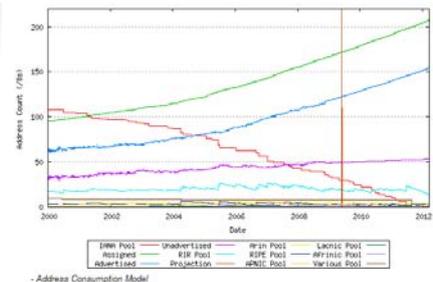
2011년 2월 23일, 전 세계 신규 IPv4 주소가 할당이 중지된다는 예측이 나오고 있는데 국내에서도 현재 사용중인 네트워크 및 보안 장비들의 IPv6 주소 지원 여부 확인 및 필요시 S/W 업그레이드나 장비 교체를 진행해야 할 시기에 이르렀습니다.

참고로, 일반 PC의 경우 OS의 업그레이드만(Windows 2000 이상)으로도 IPv6 주소를 수용할 수 있으며, IPv6 주소를 위해 LAN 카드의 추가 구입 및 교체는 불필요합니다.



• 2011년 2월 23일 [ 68일 ]

<전세계 IPv4 주소 신규 할당 중단 예상 시점 - 출처 : 한국인터넷진흥원>



• 10대 “로우키크녀” 학교 홈페이지 해킹

6살 남자 어린이를 고의로 넘어뜨려 앞니 두 개를 부러지게 한 10대 “로우키크녀” 사건으로 인해 가해자가 재학 중인 경기도 모 중학교 홈페이지를 해킹한 일이 있었습니다. 해킹으로 인해 학교 로고가 로우키크녀 사진으로 변조되었고, 이번에도 DC인사이드 코미디 갤러리 이용자들이 학교 홈페이지를 해킹한 것으로 추측되고 있습니다.



정의를 위한 익명의 헌신

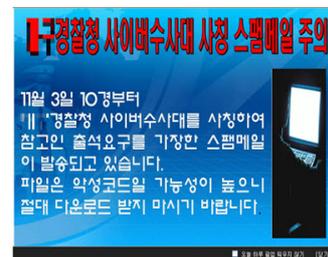
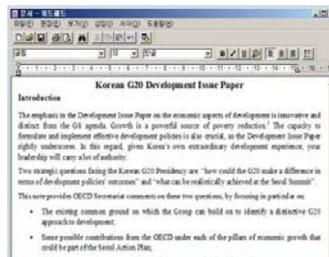


<해킹으로 변조된 학교 홈페이지 화면, 이번 해킹을 주도한 것으로 보이는 DC 코깬>

• 지방경찰청 사이버수사대, 노벨평화상 초청장을 위장한 악성코드 이메일 유포

11월에는 지방경찰청 사이버 수사대, 노벨평화상 시상식 초청장, G-20 이슈 문서를 위장한 악성코드 이메일 유포가 연이어 발생하였습니다.

사회적 이슈를 노린 전형적인 사회공학 기법의 악성코드 이메일들로 출처가 불분명한 메일은 반드시 읽지 말고 삭제해야 하며, 노벨평화상 시상식 초대장처럼 PC에 설치된 프로그램의 취약점을 이용하기는 경우도 있으므로 보안 패치들을 꼭 설치해야 합니다.



• 북한도 컴퓨터 해킹이 골치 거리 - “날래 해킹 막으랴우~ 동무!”

최근 북한에서 입수된 “북한사법일꾼을 위한 참고서”에서는 해킹과 바이러스 유포 사건이 외부와 단절된 북한에서도 일어나고 있으며, 실제 범죄 사례들을 소개하고 있습니다. 평양제1중학교에 재학 중인 김명수 학생은 자신이 만든 바이러스를 유포시켜 처벌을 받았으며, 평양 교육기관 정보센터의 박송학 연구사는 자신의 승진을 위해 해킹을 이용했지만 끝내 적발되어 2년의 노동교화형(강제노동과 노동) 처벌을 받았습니다.



<근무 시간 중 탄짓은 바로 아오지 탄광행 - “그 분이 지켜보고 있다”>

Part II 11월의 이슈 돋보기

2. 11월의 취약점 이슈

• Microsoft 11월 정기 보안 업데이트

Microsoft Office 원격코드 실행 문제점과 Forefront Unified Access Gateway의 권한 상승 문제점 등을 해결한 Microsoft 11월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- Microsoft Office XP~2010
- Microsoft Forefront Unified Access Gateway 2010

<취약점 목록>

**Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2423930)**

이 보안 업데이트는 Microsoft Office의 공개된 취약점 1건과 비공개로 보고된 취약점 4건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 특수하게 조작된 RTF 메일 메시지를 열거나 미리 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

**Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2293386)**

이 보안 업데이트는 비공개적으로 보고된 취약점 2건을 해결합니다. 사용자가 특수하게 조작된 PowerPoint 파일을 열면 이러한 Microsoft Office 취약점을 통해 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 어느 것이든 성공적으로 악용한 경우 공격자는 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

**Forefront UAG(Unified Access Gateway)의 취약점으로 인한 권한 상승 문제점(2316074)**

이 보안 업데이트는 Forefront UAG(Unified Access Gateway)에서 비공개적으로 보고된 취약점 4건을 해결합니다. 이 중 가장 심각한 취약점으로 인해 사용자가 특수하게 조작된 URL을 사용하여 영향 받는 웹 사이트를 방문할 경우 권한 상승이 허용될 수 있습니다. 그러나 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://www.microsoft.com/korea/technet/security/Bulletin/ms10-oct.msp>

영문 : <http://www.microsoft.com/technet/security/Bulletin/ms10-oct.msp>

• **Adobe Acrobat 계열 제품 보안 업데이트 권고**

Adobe Acrobat 제품군에 대한 코드 실행, DoS(Denial of Service) 보안 취약점을 패치하는 업데이트가 발표되었습니다. 특히 Adobe Acrobat 제품의 CVE-2010-3654, CVE-2010-4091 취약점을 악용하는 악성코드가 발견되었으므로 반드시 보안 업데이트를 설치하시기 바랍니다.

<해당 제품>

- Adobe Reader 9.4 이하 버전 (Windows, Mac OS, Unix)
- Adobe Acrobat 9.4 이하 버전 (Windows, Mac OS)

<취약점 목록>

메모리 손상으로 인한 DoS 공격과 코드 실행 취약점 (CVE-2010-3654)  
 메모리 손상으로 인한 DoS 공격과 코드 실행의 가능성이 있는 취약점 (CVE-2010-4091)  
 이번 취약점으로 인해 시스템 충돌(Crash)나 공격자가 시스템을 제어할 수 있습니다.

<해결책>

Adobe Flash와 Acrobat 계열 제품을 Adobe 홈페이지에서 최신으로 업데이트하거나 개별 패치를 다운로드하여 설치합니다.

최신 업데이트 사이트

Adobe Reader : <http://get.adobe.com/kr/reader/>

<참고 사이트>

<http://www.adobe.com/support/security/bulletins/apsb10-28.html>

• **Internet Explorer 원격코드 실행 제로데이 취약점 (12월 정기 보안 패치에 해결)**

CVE Number : CVE-2010-3962

인터넷 익스플로러 6~8 버전이 설치된 사용자가 악의적인 웹 사이트에 방문하면 원격의 공격자는 IE의 보안 취약점을 악용하여 임의의 코드를 실행할 수 있습니다.

<해당 제품>

- Internet Explorer 6~8 버전 (Windows XP/Vista/7)
- ※ Internet Explorer 9는 이번 취약점에 해당하지 않음

<취약점 설명>

mshtml.dll 모듈에서 CSS(Cascading Style Sheets)의 "clip" attribute를 처리할 때 브라우저의 Crash나 원격코드를 실행시킬 수 있는 취약점이 발견되었습니다.

<해결책>

12월 MS 정기 보안 패치를 설치합니다.

<참고 사이트>

한글 : <http://www.microsoft.com/korea/technet/security/Bulletin/ms10-dec.msp>

영문 : <http://www.microsoft.com/technet/security/Bulletin/ms10-dec.msp>

Contact us...

### (주)이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : [help@alyac.co.kr](mailto:help@alyac.co.kr)

알약 사이트 : [www.alyac.co.kr](http://www.alyac.co.kr)

**알약 2.5 출사기념**  
**황금알약을 잡아라!!**

알약과 함께 황금알약을 찾아 떠나보세요~

강력한 탐지력은 그대로~ 더욱 빠르고 가벼워진 알약 2.5 출시를 기념하여 푸짐한 이벤트를 마련하였습니다. 알약은 악성코드와 바이러스를 잡고, 여러분은 황금알약과 해외여행상품권을 잡아보세요!

- 기간 : 2010년 11월 8일 ~ 2010년 12월 31일
- 대상제품 : 기업용/공공기관용 알약, 알툴즈 통합보안팩

**Event 1**  
**황금알약을 잡아라!**

황금알약 받으시고 2011년엔 더 대박나세요~

- 대상 : 200만원 이상 구매고객 모두
- 내용 : 순금알약 핸드폰 액세서리 1/2 돈 증정 (구매금액 200만원당 1개씩)

**Event 2**  
**여행상품권을 잡아라!**

올 겨울 따뜻한 남쪽 나라로 떠나보세요~

- 대상 : 5user 이상 구매고객 모두
- 내용 : 추첨을 통해 매월 3명에게 50만원 여행상품권 2매 증정

**이벤트 응모하기**      **당첨자 확인**

**안내사항**

- 여행상품권 당첨자는 매월 말 알약 홈페이지에 공지됩니다.
- 여행상품권 응모방법은 이벤트 응모페이지를 참고하시기 바랍니다.
- 황금알약 경품은 이벤트 기간 중 구매하신 총 금액을 기준으로 1회만 제공됩니다.
- 황금알약 경품은 매월 초에 일괄배송됩니다.

알툴즈&알집 구매 고객을 대상으로 "두마리 토끼를 잡아라!" 이벤트도 함께 진행 중입니다. <http://www.altools.co.kr>